Deutscher Bundestag **Drucksache 18/7183**

18. Wahlperiode 30.12.2015

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Frank Tempel, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/7024 –

Europäische Anstrengungen zur möglichen Aushebelung verschlüsselter Telekommunikation

Vorbemerkung der Fragesteller

Im November 2015 hat der luxemburgische Ratsvorsitz ein Papier mit einem Sachstand an die Mitgliedstaaten verschickt, in dem Herausforderungen durch die „Kommunikationskanäle des Internets und die zahlreichen sozialen Medien" skizziert werden (Ratsdok. 14677/15). Neue „verschlüsselungsbasierte Technologien" würden die „Durchführung effektiver Ermittlungen" zunehmend erschweren oder verhindern. Von besonderer Bedeutung seien diese auch bei „Antiradikalisierungsmaßnahmen". Das Papier fordert unter anderem eine „effektive Vorratsdatenspeicherung". In einem weiteren Dokument fragt der luxemburgische Ratsvorsitz den Bedarf für entsprechende Schritte der Kommission ab (Ratsdok. 14369/15). Als weitere Hindernisse für Strafverfolger werden die „private Nutzung des Live-Streamings", das Darknet und Anonymisierungswerkzeuge genannt. „Entscheidende elektronische Beweismittel" gingen verloren, wenn den zuständigen Behörden keine geeigneten Mittel zur Verfügung gestellt würden.

Im Januar 2015 forderte der EU-Anti-Terror-Koordinator Gilles de Kerchove, Internet- und Telekommunikationsanbieter zum Einbau von Hintertüren für verschlüsselte Kommunikation zu zwingen (www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf). Im März 2015 warnte der Direktor des Europäischen Polizeiamtes (Europol), Rob Wainwright, vor der zunehmenden Nutzung von Verschlüsselungstechnologien. Verschlüsselung sei demnach „eines der Hauptinstrumente von Terroristen und Kriminellen". Im September 2015 trug der stellvertretende Leiter der Operationsabteilung von Europol, Wil van Gemert, auf einer Konferenz der europäischen Polizeichefs den Bericht einer Arbeitsgruppe zu „terroristischen Online-Bedrohungen" vor (www.statewatch.org/news/2015/nov/eu-council-eppc-2015-report-09-2015.pdf). Demnach müssten vor allem die „Hindernisse von Anonymisierung und Verschlüsselung" überwunden werden. An der Arbeitsgruppe nahmen unter anderem Behörden aus Österreich, Dänemark, Ungarn, Deutschland und Spanien teil. Sie raten zu mehr Kooperation mit dem „privaten Sektor", darunter Providern und Diensteanbietern, um an verschlüsselte Inhalte und den Zugang zu Servern zu gelangen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 28. Dezember 2015 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Zum zweiten Mal hat Europol im Herbst einen Lagebericht zu Cyberkriminalität herausgegeben, in dem das Thema Verschlüsselung und Anonymisierung ausführlich behandelt wird (www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015). Zu den Erschwernissen für die Behörden zählt Europol auch „Anti-Forensik-Werkzeuge“, darunter Software zum Überschreiben von Inhalten oder Betriebssysteme, die von Wechselmedien gestartet werden. Diese seien bei Kriminellen nicht mehr die Ausnahme, sondern die Regel. In Ermittlungen würden jedoch in „zunehmendem Ausmaß“ digitalisierte Daten benötigt. Laut Europol seien die Ermittlerinnen und Ermittler in drei Vierteln aller Fälle mit verschlüsselten Inhalten konfrontiert. Namentlich genannt werden die Anwendungen TrueCrypt und BitLocker sowie PGP, dessen zunehmende Nutzung von den Behörden der Mitgliedstaaten bestätigt worden sei. Internetanbieter und Plattformen wie WhatsApp, iMessage, Facebook, Facetime, Google und Yahoo würden zudem die voreingestellte Ende-zu-Ende-Verschlüsselung implementieren. Zwar sei dies für den „öffentlichen und privaten Sektor“ zu begrüßen, jedoch stelle sich die Frage nach der Bedeutung dieser Entwicklung für Regierungen und Strafverfolgungsbehörden.

Der Bericht schlägt mehrere Maßnahmen vor. „Gesetzgeber“ und Abgeordnete müssten „mit der Industrie und der Forschung“ brauchbare Lösungen entwickeln, die einerseits die Privatheit und Urheberrechte respektieren, den Behörden jedoch ausreichend Handhabe zur Bekämpfung von „kriminellen oder nationalen Sicherheitsbedrohungen“ bereitstellten. Auch Ermittlungen wegen Kinderpornografie seien hiervon betroffen. Zu den Empfehlungen gehört die Entwicklung von Techniken, um bei einer polizeilichen Razzia Daten aus verschlüsselten, aber noch nicht ausgeschalteten Systemen rekonstruieren zu können. Die Behörden sollten außerdem eine „zentrale Datenbank“ mit „VPN- und Proxy-Diensten“ anlegen, die bevorzugt von „Cyberkriminellen“ genutzt würden.

Nun will sich auch die Gruppe „Freunde der Präsidentschaft zu Cyber“ (FoP Cyber) mit dem Umgehen von Verschlüsselung befassen (www.statewatch.org/news/2015/dec/eu-council-cosi-int-sec-14079-15.pdf). Auch dort ist die Rede von Ermittlungshindernissen, die es zu überwinden gelte. Die Gruppe kündigt an, die zukünftige Entwicklung im Auge zu behalten. Jeder teilnehmende Mitgliedstaat entsendet einen „Cyber-Attaché“ nach Brüssel. In den zwei letzten Treffen dieser hohen Beamtinnen und Beamten im Oktober und November 2015 ging es unter anderem um den „Missbrauch von Verschlüsselung und Anonymität“ und entsprechende Gesetzeslücken. Die Gruppe will nun für öffentliches Bewusstsein zum Thema sorgen, Handlungsempfehlungen geben und die Kommission mit „praktischen Beiträgen“ zu neuen Gesetzgebungsvorschlägen versorgen.

Im Bundesministerium des Inneren werden die europäischen Anstrengungen ausdrücklich begrüßt (Bundestagsdrucksache 18/5144). Das „Streben nach einer abgeschirmten, klandestinen Übermittlung von Informationen“ sei in vielen Phänomen- und Kriminalitätsbereichen ein „prägendes Wesensmerkmal im Kommunikationsverhalten“. Dieses hätte zum Ziel, „die staatlichen Aufklärungs- und Bekämpfungsmaßnahmen ins Leere laufen zu lassen“. Für den Zugriff auf nutzerseitig verschlüsselte Kommunikation bestehe jedoch derzeit keine Rechtsgrundlage. Zur Suche nach den „unterschiedlichen Bedürfnissen im Verhältnis Datenschutz zu Gefahrenabwehr und Strafverfolgung“ sei deshalb „jedweder Dialog mit Internet-Diensteanbietern“ zu begrüßen. Als nächsten Schritt hat die EU am 3. Dezember 2015 den offiziellen Start des „Forums der Internetdienstleister“ verkündet. In der neuen Gemeinschaft organisieren sich die EU-Innenministerinnen und EU-Innenminister mit Internetkonzernen. Nach über einem Jahr Vorbereitung wird eine Zusammenarbeitsform installiert, die eine möglichst schnelle Beseitigung unliebsamer Internetinhalte ermöglichen soll. Zu den weiteren „Möglichkeiten der praktischen Zusammenarbeit“ zählt der Umgang mit Verschlüsselungstechniken.

1. Inwiefern sieht auch die Bundesregierung neue Herausforderungen durch die „Kommunikationskanäle des Internets und die zahlreichen sozialen Medien“ hinsichtlich „verschlüsselungsbasierter Technologien“ und deren Verhinderung der „Durchführung effektiver Ermittlungen“?

Auf die Antwort der Bundesregierung zu Frage 5 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/5144 vom 11. Juni 2015 wird verwiesen.

2. Wie hat sich die Bundesregierung zu einem entsprechenden Papier des luxemburgischen Ratsvorsitzes positioniert?

Die Bundesregierung geht aufgrund der Zitate in den Fragen 1 und 3 davon aus, dass die Fragesteller das Ratsdokument 14369/15 meinen (abrufbar unter http://data.consilium.europa.eu/doc/document/st-14369-2015-init/de/pdf). Die Bundesregierung hat das Papier des luxemburgischen Ratsvorsitzes zur Kenntnis genommen. Eine aktive Kommentierung oder ein Redebeitrag ist hierzu seitens der Bundesregierung nicht erfolgt.

3. Welche „Antiradikalisierungsmaßnahmen“ sind nach Kenntnis der Bundesregierung in dem Papier gemeint?

Den Ausführungen des luxemburgischen Ratsvorsitzes lassen sich keine Bezüge zu konkreten Antiradikalisierungsmaßnahmen entnehmen.

4. Wie hat sich die Bundesregierung gegenüber dem Ratsvorsitz zur Frage des Auftrages der Kommission hinsichtlich der Vorratsdatenspeicherung positioniert, und wie wurden die Fragen des versandten Fragebogens beantwortet?

Die im Ratsdokument 14677/15 enthaltenen Fragen wurden bei der Sitzung des Rates für Justiz und Inneres am 3./4. Dezember 2015 diskutiert. Die Bundesregierung ist der Ansicht, dass eine anlasslose verpflichtende Speicherung von Verkehrsdaten zulässig ist, wenn sie strengen Anforderungen hinsichtlich des Umfangs der gespeicherten Daten sowie der Datenverwendung unterliegt und auf das absolut Notwendige beschränkt wird. Hinsichtlich der Datensicherheit muss ein hoher Standard normenklar und verbindlich vorgegeben werden. In diesem Sinne hat sich die Bundesregierung zur im Ratsdokument 14677/15 genannten Frage 1 geäußert. Zu den Fragen 2 und 3 hat die Bundesregierung ihre Position zu bedenken gegeben, die Frage, ob eine europäische Neuregelung angestrebt werden soll, zunächst zurückzustellen und die Entscheidung des Gerichtshofs der Europäischen Union in der Rechtssache Tele2 Sverige AB (schwedisches Vorabentscheidungsersuchen, C-203/15) abzuwarten.

5. Welche Behörden (auch deutsche) haben nach Kenntnis der Bundesregierung an einer Arbeitsgruppe zu „terroristischen Online-Bedrohungen“ teilgenommen?

An der Arbeitsgruppe hat für Deutschland das Bundeskriminalamt teilgenommen. Daneben haben Vertreter aus Österreich, Bulgarien, Belgien, Italien, der Tschechischen Republik, Dänemark, Finnland, Frankreich, Ungarn, Spanien und dem Vereinigten Königreich sowie von Europol teilgenommen.

a) Auf welche Weise hat sich diese Arbeitsgruppe auch mit Anonymisierung und Verschlüsselung befasst?

Die Arbeitsgruppe hat erörtert, in welcher Weise Anonymisierung und Verschlüsselung die Bemühungen der Strafverfolgungsbehörden zur Ermittlung von Tätern und Tatverdächtigen erschweren und wie eine Zusammenarbeit mit der Privatwirtschaft insoweit hilfreich sein kann.

b) Welche weiteren Teilnehmenden (auch zur Beratung) waren eingebunden?

Nach Kenntnis der Bundesregierung waren keine weiteren Teilnehmer eingebunden.

c) Wie lange soll die Arbeitsgruppe bestehen?

Die Arbeitsgruppe bestand nur für die Zeit der Vorbereitung der diesjährigen „European Police Chiefs Convention“ am 23./24. September 2015.

6. Welche konkreten Vorschläge zur Überwindung entsprechender „Hindernisse“ werden in dem Bericht der Arbeitsgruppe gemacht?

Auf die Antwort zu Frage 5a wird verwiesen.

a) Sofern zu mehr Kooperation mit Providern und Diensteanbietern geraten wird, um an verschlüsselte Inhalte und den Zugang zu Servern zu gelangen, wie könnte dies aus Sicht der Bundesregierung umgesetzt werden?

Zur Frage der Kooperation mit Providern und Diensteanbietern wird auf die Antworten zu den Fragen 10 und 11 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/5144 vom 11. Juni 2015 verwiesen.

b) Welche Schlussfolgerungen zieht die Bundesregierung aus dem Bericht, und welchen der dort vorgeschlagenen Maßnahmen stimmt sie zu?

Die Bundesregierung stimmt allen im Abschlussbericht dieser Arbeitsgruppe vorgeschlagenen Empfehlungen zu.

c) Was ist nach Kenntnis der Bundesregierung damit gemeint, wenn Europol fordert, eine „zentrale Datenbank“ mit „VPN- und Proxy-Diensten“ anzulegen, und wo könnte diese angesiedelt werden?

Nach der Vorbemerkung der Fragesteller handelt es sich um eine Aussage aus dem „2015 Internet Organised Crime Threat Assessment“ (IOCTA) von Europol. Der Bundesregierung liegen keine darüber hinausgehenden Erkenntnisse zum Hintergrund dieser Forderung von Europol vor.

7. Inwiefern stehen auch Bundesbehörden vor dem Problem der zunehmenden Verwendung von „Anti-Forensik-Werkzeugen“, darunter Software zum Überschreiben von Inhalten oder Betriebssysteme, die von Wechselmedien gestartet werden?

Die Ermittlungsbehörden des Bundes konnten bisher in wenigen Einzelfällen eine Nutzung von „Anti-Forensik-Werkzeugen“, darunter Software zum Überschreiben von Inhalten oder Betriebssystemen, die von Wechselmedien gestartet werden, feststellen. Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

8. In welcher Größenordnung sind deutsche Behörden nach Kenntnis der Bundesregierung mit verschlüsselten Inhalten konfrontiert?

Statistiken über den Umfang der Konfrontation der Behörden des Bundes mit gespeicherten verschlüsselten Inhalten werden seitens der Bundesregierung nicht geführt. Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

9. Welche der Werkzeuge werden dabei besonders häufig eingesetzt?

Es wird auf die Antwort zu Frage 8 verwiesen. Die in der Vorbemerkung der Fragesteller zitierten Feststellungen von Europol decken sich im Wesentlichen mit den Erkenntnissen der Bundesregierung.

10. Auf welche Weise hat sich nach Kenntnis der Bundesregierung die Gruppe „FoP Cyber“ mit dem Thema Verschlüsselung befasst?

In der Sitzung der Gruppe „Freunde der Präsidentschaft zu Cyber“ (FoP) am 11. November 2015 wurde in einer Präsentation des European Cybercrime Centre (Europol EC3) „Gaps in the Fight against Cybercrime: Case Study“ auf die zunehmende Verschleierung von kriminellen Handlungen, Identitäten und Tatorten durch verschlüsselte Kommunikation hingewiesen.

11. Auf welche Weise und mit welchen Initiativen und Maßnahmen will die FoP Cyber das Thema weiter behandeln?

Nach Kenntnis der Bundesregierung wurde das Thema bisher nicht auf die Tagesordnung für folgende Sitzungen der FoP gesetzt.

12. Welche Mitgliedstaaten oder sonstigen Teilnehmenden haben einen „Cyber-Attaché“ zur FoP Cyber entsandt?

Die FoP ist ein vom Rat eingesetztes Arbeitsgremium, an dessen Sitzungen alle EU-Mitgliedstaaten teilnehmen und das im Hauptstadtformat, also mit Bediensteten aus den Hauptstädten, tagt. Außer den Sitzungen der FoP gibt es Treffen im Brüsseler „Attaché-Format“, an denen die Mitgliedstaaten mit Bediensteten ihrer Ständigen Vertretungen bei der EU teilnehmen. Für dortige Bedienstete, zu deren Aufgabenportfolio die Vertretung ihres Staates in den Attaché-Sitzungen gehört, hat sich inoffiziell die Bezeichnung „Cyber-Attaché“ eingebürgert.

13. In welchen Treffen der FoP Cyber hat diese nach Kenntnis der Bundesregierung das Thema Verschlüsselung behandelt, und wer trug dazu vor (bitte auch das Thema der Präsentationen benennen)?

Auf die Antwort zu Frage 10 wird verwiesen.

a) Welche „Gesetzeslücken“ wurden identifiziert?

Im Rahmen des in der Antwort zu Frage 10 genannten Vortrags wurde die Frage möglicher Gesetzeslücken nicht behandelt.

b) In welchen weiteren Treffen steht das Thema auf der Tagesordnung?

Auf die Antwort zu Frage 11 wird verwiesen.

14. Aus welchen Erwägungen nehmen nach Kenntnis der Bundesregierung auch der für die Sicherheits- und Verteidigungspolitik zuständige Europäische Auswärtige Dienst (EAD) sowie die Europäische Verteidigungsagentur (EDA) an der FoP Cyber teil?

Gemäß dem vom Rat erteilten Arbeitsauftrag gehört es zu den Aufgaben der FoP, cyberpolitische Fragestellungen aus einer über Einzelthemen hinausgehenden EU-Gesamtperspektive zu betrachten, den Informationsaustausch zwischen den diversen Cyberpolitik-Akteuren innerhalb der EU und in den EU-Mitgliedstaaten zu fördern und zur Vermittlung kohärenter cyberpolitischer Botschaften gegenüber Drittstaaten beizutragen. Die fallweise Teilnahme an FoP-Sitzungen vom Europäischen Auswärtigen Dienst (EAD), der Europäischen Verteidigungsagentur (EDA) und von weiteren EU-Institutionen stellt sicher, dass die FoP das angestrebte cyberpolitische Gesamtbild erstellen kann.

15. Auf welche Weise sollten bzw. könnten der EAD und die EDA aus Sicht der Bundesregierung das Thema Verschlüsselung behandeln?

Eine Befassung mit dem Thema Verschlüsselung ist aus Sicht der Bundesregierung im Rahmen der regulären Aufgabenwahrnehmung von EAD (im Rahmen der beschlossenen „Cyber-Diplomatie“ gegenüber Drittstaaten) oder EDA (Umsetzung beschlossener Projekte zu „Cyber Defense“) denkbar.

16. Auf welche Weise will die FoP Cyber nach Kenntnis der Bundesregierung für öffentliches Bewusstsein zum Thema sorgen, Handlungsempfehlungen geben und die Kommission mit „praktischen Beiträgen“ zu neuen Gesetzgebungsvorschlägen versorgen?

Die FoP arbeitet auf der Grundlage des vom Rat beschlossenen Arbeitsauftrags. Im Übrigen wird auf die Antwort zu Frage 14 verwiesen.

17. Welche Haltung vertritt die Bundesregierung hinsichtlich der Notwendigkeit neuer Regelungen zur Sicherstellung von digitalen Beweismitteln „e-evidence“?

Die Sicherstellung von Gegenständen zu Beweiszwecken ist in § 94 der Strafprozessordnung (StPO) geregelt. Gegenstände im Sinne dieser Vorschrift sind auch digital gespeicherte Informationen. Die Bundesregierung sieht insoweit keinen Bedarf für eine Neuregelung.

a) Inwiefern sollte hierzu auch die Übermittlung von Daten durch Internetanbieter zu Polizeien und Geheimdiensten erleichtert werden?

Auf die Antwort zu Frage 17 wird verwiesen.

b) Inwiefern sieht die Bundesregierung entsprechende Defizite auch in der grenzüberschreitenden Zusammenarbeit mit den USA, und auf welche Weise wird das Thema in den nächsten Monaten behandelt?

Die Bundesregierung sieht hinsichtlich der grenzüberschreitenden Zusammenarbeit mit den USA im Bereich „e-evidence“ keinen aktuellen Regelungsdarf.

c) Was ist der Bundesregierung darüber bekannt, inwiefern die US-Regierung mit EU-Mitgliedstaaten darüber verhandeln möchte oder bereits verhandelt, dass US-Strafverfolger zukünftig bei EU-Internetanbietern Auskunftsverlangen zu Telekomunikationsdaten stellen und womöglich auch die Echtzeit-Telekommunikationsüberwachung verlangen dürfen?

Die Bundesregierung verfügt zur Frage, inwiefern die US-Regierung mit EU-Mitgliedstaaten darüber verhandeln möchte oder bereits verhandelt, dass US-Strafverfolger zukünftig bei EU-Internetanbietern Auskunftsverlangen zu TK-Daten stellen und womöglich auch die Echtzeit-Telekommunikationsüberwachung verlangen dürfen, über keine Erkenntnisse. Im Übrigen wird auf die Antwort zu Frage 17b verwiesen.

18. Wie viele Ersuchen zur Entfernung von Internetinhalten hat die „Meldestelle für Internetinhalte“ bei Europol nach Kenntnis der Bundesregierung bereits erhalten, und wie vielen der Ersuchen wurde nachgekommen?

Im Zeitraum vom 15. Juli 2015 bis zum 11. November 2015 wurden von Europol und durch Meldungen der Mitgliedstaaten 920 Internetinhalte für eine potentielle Meldung an den betroffenen Internetdienstleister identifiziert. Davon wurden 493 Inhalte bereits den betroffenen Internetdienstleistern gemeldet. In 314 Fällen haben die betroffenen Internetdienstleister entschieden, den Inhalt aus ihrem Angebot zu entfernen.

19. Inwiefern wird auch die Bundesregierung dem Aufruf der “Meldestelle” nachkommen, mehr „nationale Experten“ zu entsenden?

Bislang hat die Bundesregierung keinen nationalen Experten zur „Meldestelle“ entsandt. Über eine etwaige künftige Entsendung ist noch keine Entscheidung getroffen.

20. Welche privaten Teilnehmenden des am 3. Dezember 2015 in Brüssel gestarteten „Forums der Internetdienstleister“ sind der Bundesregierung durch ihre eigene Teilnahme bekannt (Plenarprotokoll 18/142), und aus welchem Grund wurden entgegen früheren Ankündigungen der Kommission keine Vertreter der Zivilgesellschaft eingeladen (Antwort der Kommission auf die Anfrage von Cornelia Ernst, MEP, Kommissionsdokument E-006551/2015)?

Gegenüber den Angaben im Plenarprotokoll 18/142, Anlage 16, in der Antwort auf die Mündliche Frage 17 des Abgeordneten Andrej Hunko ergibt sich kein Ergänzungsbedarf. Die Auswahl und Einladung der Teilnehmer liegt in der ausschließlichen Verantwortung der Europäischen Kommission.

21. Inwiefern hält auch die Bundesregierung die Teilnahme von Vertretern der Zivilgesellschaft für entbehrlich?

Nach Kenntnis der Bundesregierung beabsichtigt die Europäische Kommission, Vertreter der Zivilgesellschaft je nach Themenschwerpunkt von Fall zu Fall zu ggf. stattfindenden zukünftigen Treffen des „Forums der Internetdienstleister" einzuladen. Im Übrigen wird auf die Antwort zu Frage 20 verwiesen.

22. Welche Veränderungen werden sich aus Sicht der Bundesregierung durch die Umwandlung des „Radicalisation Awareness Network" in ein „Centre of Excellence" für die Arbeit des Zentrums ergeben?

Mit Wirkung vom 1. Oktober 2015 wurde das Aufklärungsnetzwerk gegen Radikalisierung (Radical Awareness Network – RAN) durch die Europäische Kommission in ein Exzellenzzentrum (Center of Excellence – CoE) umgewandelt, dessen vollständige Funktionsfähigkeit durch die Europäische Kommission für Januar 2016 avisiert wurde. Durch die Umwandlung in ein CoE soll das bisherige Sekretariat in seiner Arbeit gestärkt werden. Zudem ist damit eine Aufstockung der Mittel seitens der Europäischen Kommission verbunden. Das CoE wird die Unterstützung des Netzwerks von Praktikern fortsetzen. Es wird ebenfalls weitere Aufgaben wie z. B. die Koordination von am Bedarf der Praktiker ausgerichteten Forschungsprojekten, die Veröffentlichung von themenbezogenen Papieren oder die bedarfsgerechte Beratung von Mitgliedstaaten fortführen. Zusätzlich zu seiner logistischen Rolle innerhalb des RAN soll das CoE künftig auch als zentrale Stelle bei der Vernetzung, Entwicklung und Verbreitung von Expertise – und damit nach Aussage der Europäischen Kommission verstärkt auch als eine Art thinktank – fungieren.

23. Bei welchen vorbereitenden Treffen des am 3. Dezember 2015 gestarteten „Forums der Internetdienstleister" wurde das Thema Verschlüsselung nach Kenntnis der Bundesregierung behandelt, und wer trug dazu vor (bitte auch das Thema der Präsentationen benennen)?

    a) Welche „Möglichkeiten der praktischen Zusammenarbeit" wurden dabei bislang behandelt, und inwieweit hält die Bundesregierung diese für praktikabel?

Die Fragen 23 und 23a werden gemeinsam beantwortet.

Nach Kenntnis der Bundesregierung wurde das Thema Verschlüsselung bei keinem vorbereitenden Treffen des am 3. Dezember 2015 gestarteten „Forums der Internetdienstleister" behandelt.

    b) Was ist der Bundesregierung darüber bekannt, auf welchen zukünftigen Treffen das Thema Verschlüsselung behandelt werden soll?

Der Bundesregierung ist nicht bekannt, ob und auf welchen ggf. stattfindenden zukünftigen Treffen des „Forums der Internetdienstleister" das Thema Verschlüsselung behandelt werden soll.

24. Was ist der Bundesregierung über Pläne bekannt, die am Forum teilnehmenden Internetanbieter dafür zu gewinnen, bei besonderen terroristischen Vorkommnissen die Schaltung von Werbung gratis anzubieten, um möglichst viele „Gegendiskurse" produzieren zu können, und welche Haltung vertritt sie hierzu?

Nach Ansicht der Bundesregierung ist auch eine Zusammenarbeit zwischen Zivilgesellschaft und Internetunternehmen bei der Bekämpfung des gewalttätigen Extremismus und von Hasskommentaren wichtig und wünschenswert.

Nach Kenntnis der Bundesregierung haben sich im Rahmen der vom Bundesministerium der Justiz und für Verbraucherschutz eingerichteten Task Force „Umgang mit rechtswidrigen Hassbotschaften im Internet" mehrere Internetunternehmen bereiterklärt, die an der Task Force beteiligten zivilgesellschaftlichen Organisationen (Amadeu-Antonio-Stiftung (Netz gegen Nazis), Gesicht zeigen! e. V., eco – Verband der Internetwirtschaft e. V., Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM), jugendschutz.net, klicksafe.de) auch durch die Bereitstellung von Werbeplätzen bei ihrer Arbeit zu unterstützen. Ein Zusammenhang mit „besonderen terroristischen Vorkommnissen" besteht dabei nicht.

25. Was ist der Bundesregierung darüber bekannt, welche großen US-Internetdienstleister personenbezogene Nutzerdaten, IP-Adressen oder Informationen über besuchte Webseiten auch ohne Rechtshilfeersuchen herausgeben?

Im Rahmen ihrer gesetzlichen Zuständigkeiten können deutsche Strafverfolgungs- und Sicherheitsbehörden auf Antrag von einigen US-Internetdienstleistern Auskunft über Bestandsdaten von Nutzern („subscriber information") im Einzelfall erhalten. Die Auskunftserteilung durch diese US-Internetdienstleister erfolgt auf der Grundlage der Anerkennung der gesetzlichen Befugnisse und Zuständigkeiten der deutschen Strafverfolgungs- und Sicherheitsbehörden und im Einklang mit den Nutzungsbedingungen der Internetdienstleister und der deutschen und US-amerikanischen Rechtsordnung.

Darüber hinausgehende Informationen, also insbesondere Kommunikationsinhalte, werden von diesen US-Internetdienstleistern nur auf der Grundlage eines Rechtshilfeersuchens herausgegeben.

26. Welche Haltung vertritt die Bundesregierung zu der Frage, ob der Zugang großer US-Internetdienstleister in europäischen Märkten an die Frage der Herausgabe personenbezogener Nutzerdaten gekoppelt sein sollte?

Eine Kopplung des Zugangs großer US-Internetdienstleister zum europäischen Markt an die Frage der Herausgabe personenbezogener Nutzerdaten wird von der Bundesregierung nicht verfolgt.

27. Was ist der Bundesregierung über Forderungen einzelner EU-Mitgliedstaaten nach einem generellen Verbot von Verschlüsselung bekannt, und welche Auswirkungen hätte dies auf die deutsche Haltung zu Verschlüsselung?

28. Was ist der Bundesregierung über Forderungen einzelner EU-Mitgliedstaaten bekannt, wonach alle Anbieter von Verschlüsselungstechnologien zur Einrichtung von Hintertüren für Strafverfolger gezwungen werden sollten, und welche Auswirkungen hätte dies auf die deutsche Haltung zu Verschlüsselung?

Die Fragen 27 und 28 werden gemeinsam beantwortet.

Der Bundesregierung ist die Debatte über denkbare Formen der Regulierung von Verschlüsselung bekannt. Zur Haltung der Bundesregierung im Hinblick auf Verschlüsselung wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 21 des Abgeordneten Dr. Konstantin von Notz auf Bundestagsdrucksache 18/6760 verwiesen.

29. In welchen der oben genannten Zusammenarbeitsformen wurde nach Kenntnis der Bundesregierung auch thematisiert, den gewünschten Zugang von Strafverfolgungsbehörden zu verschlüsselter Telekommunikation durch den verstärkten (grenzüberschreitenden) Einsatz staatlich genutzter Trojanerprogramme zu ermöglichen?

    a) Wer trug hierzu entsprechende Ausführungen vor?

    b) Inwiefern wurde bei den Vorträgen und Diskussionen auch über EU-weit oder international zu vereinheitlichende Regelungen verwiesen, und um welche handelt es sich dabei?

Die Fragen 29 bis 29b werden gemeinsam beantwortet.

Nach Kenntnis der Bundesregierung wurde in keiner der von den Fragestellern genannten Zusammenarbeitsformen der Zugang von Strafverfolgungsbehörden zu verschlüsselter Telekommunikation durch den verstärkten grenzüberschreitenden Einsatz „staatlich genutzter Trojanerprogramme“ thematisiert.

30. Auf welche Weise wäre eine EU-weit oder international zu vereinheitlichende Regelung des (grenzüberschreitenden) Einsatzes staatlich genutzter Trojanerprogramme aus Sicht der Bundesregierung eine geeignete Möglichkeit zur Umsetzung des gewünschten Zugangs von Strafverfolgungsbehörden zu verschlüsselter Telekommunikation?

Eine EU-weit oder international zu vereinheitlichende Regelung des grenzüberschreitenden Einsatzes „staatlich genutzter Trojanerprogramme“ wird von der Bundesregierung nicht angestrebt.

31. Was ist der Bundesregierung darüber bekannt, inwiefern auch die EU-Agentur Eurojust in Anstrengungen eingebunden ist, den Kontakt zu Internetdienstleistern hinsichtlich der Entfernung von Inhalten oder der Strafverfolgung zu verbessern, und welche Internetkonzerne wurden zu einem entsprechenden Treffen im Oktober 2015 eingeladen (www.statewatch.org/news/2015/nov/eu-council-c-t-implementation-strategy-14438-15.pdf)?

Der Rat der Innen- und Justizminister vom Oktober und Dezember 2015 hat Eurojust bei der Befassung mit dem Thema „Migrationskrise: Aspekte der justiziellen Zusammenarbeit und Kampf gegen Fremdenfeindlichkeit“ eine wichtige Rolle zugeschrieben, siehe Ratsdokument 12372/15 und den Follow-up-Bericht

auf Ratsdokument 14716/15. Die Mitgliedstaaten werden unter anderem aufgefordert, die Unterstützungsangebote von Eurojust angemessen zu nutzen. Eurojust arbeitet zudem mit Europol EC3 zusammen und hat einen speziellen Kontaktbeamten dazu benannt. Am öffentlichen Teil eines von Eurojust ausgerichteten EU-US-Seminars am 8./9. Oktober 2015 nahmen Vertreter von Apple, Microsoft und DIGITALEUROPE teil.

32. Wann soll die europäische Ermittlungsanordnung nach Kenntnis der Bundesregierung in nationales Recht umgesetzt werden, und inwiefern hält die Bundesregierung die in der Richtlinie geregelte grenzüberschreitende Anordnung von Zwangsmaßnahmen schon jetzt für überarbeitungswürdig?

Die Mitgliedstaaten sind nach Artikel 36 Absatz 1 der Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen (RL EEA) gehalten, die erforderlichen Umsetzungsarbeiten bis zum 22. Mai 2017 vorzunehmen. Die Bundesregierung strebt eine pünktliche Umsetzung an. Zum gegenwärtigen Zeitpunkt sieht die Bundesregierung keinen Bedarf zur Überarbeitung des Richtlinientextes.

33. Welche Priorisierungen hat die Bundesregierung in Reaktion auf das Ratsdok. 14369/15 vorgenommen (bitte die Punkte kurz anreißen)?

Das Ratsdokument war Grundlage der Beratungen des Rates der Justiz- und Innenminister am 3. und 4. Dezember 2015. Die Minister haben deutlich gemacht, dass alle in dem Dokument dargestellten Herausforderungen mit Vorrang bearbeitet werden sollen. Dies entspricht auch der Einschätzung der Bundesregierung.



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333